экспертного исследования и достижения целей предварительного расследования.

УДК 343.985

Н. С. Зиновьева

ЗАКОНОМЕРНОСТИ ОБМЕНА ИНФОРМАЦИЕЙ ПОСРЕДСТВОМ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И ИХ ИСПОЛЬЗОВАНИЕ В АНТИТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Терроризм – это глобальная проблема современности. Процесс глобализации порождает многочисленные социально-политические кризисы, противоречия и конфликты, одним из способов разрешения которых становится осуществление террористической деятельности.

Проблемой противодействия терроризму сегодня обеспокоено все международное сообщество и, конечно же, сотрудники органов внутренних дел, осуществляющие непосредственную борьбу с терроризмом.

Повышение эффективности деятельности сотрудников по раскрытию, расследованию и предупреждению преступлений при помощи современных информационно-телекоммуникационных инфраструктур, предоставило возможность сотрудникам ОВД раскрывать и расследовать в «кибернетическом мире» проявления террористической деятельности.

Мобильные устройства, платформы социальных сетей могут привести к практически всеобщей ситуационной осведомленности как террористических организаций для подготовки дисбалансирующих общественных мероприятий, так и сотрудников органов внутренних дел для предотвращения данного рода явлений.

Террористические организации могут анализировать данные, поступающие из разных источников, и способны сводить их к полезной тактической информации. Суть в том, что террористы собирают, казалось бы, безобидную информацию из многочисленных источников, в результате получая полную картину, дающую им тактическую ситуационную осведомленность.

Так, к примеру, на этапе планирования террористических акций террористические организации имеют обширную возможность для «виртуальной» разведки объектов с помощью сетевой картографической службы. В процессе непосредственной атаки террористы могут использовать сотовые телефоны для передачи информации исполнителям. Наличие смартфона и возможность приобретения зарегистрированных на подставных лиц SIM-карт во многих странах позволяют террористам использовать интернет, избегая каких-либо форм идентификации личности. Таким образом, обширные возможности использования

террористическими организациями современными телекоммуникационными системами, само собой, порождает необходимость разработки закономерного ответа по использованию сотрудниками органов внутренних дел кибернетических закономерностей управления, передачи и хранения информации в сети Интернет в целях предотвращения угроз террористического характера.

Так, для розыска преступников (террористов) в глобальной паутине Интернет сотрудникам достаточно знать уникальный IP-адрес искомого субъекта, являющийся ничем иным, как сетевым адресом абонента.

Одними из методов получения информации об IP-адресе абонента может являться поэтапная процедура запросов управляющим компаниям, услугами которых пользуется разыскиваемый субъект, или использование сотрудниками специальных программ «Снифферов», откладывающих информацию о пользователе того или иного интернет-ресурса в специальные файлы на сервере (лог сниффера).

Обладая информацией об IP-адресе пользователя интернет-ресурса, полученной одним из перечисленных способов (оперативным либо официальным), должностному лицу предоставляется возможность установить и географическое место выхода абонента в глобальную информационную сеть. Таковыми сведениями обладает провайдер.

Однако все усилия правоохранительных структур в данной сфере могут быть напрасны в виду того, что в настоящий момент либо вовсе отсутствует нормативно-правовое регулирование сроков хранения информации о пользователях интернет-ресурсов (социальных сетей, форумов и т. п.), либо такие сроки недостаточны для использования данной информации. Тем самым видим целесообразным предложить установить сроки хранения указанной информации на законодательном уровне. На наш взгляд, 3 года – это достаточный срок для проведения оперативно-розыскных мероприятий, которые позволят воспользоваться столь обширными возможностями по изобличению лиц, причастных к террористической деятельности, в «кибернетическом мире».

Таким образом, в современном мире, активно использующем телекоммуникационные средства общения, всевозрастающее значение приобретает изучение криминалистической кибернетики и использование ее достижений в раскрытии и расследовании преступлений, в том числе для реализации розыскной деятельности следователем в рамках антитеррористической деятельности.